REMARKS

Independent claims 2 and 18 have been amended for clarification. No other claim has been amended, added or deleted, and no new matter has been added. Upon entry of the above amendments, claims 2-14 and 16-21 will remain in the application.

Claim Rejections – 35 U.S.C. §103(a)

Claims 2-14 and 16-21 stand finally rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Anderson et al. (US 2003/0002436) (hereinafter "Anderson") in view of Lin et al. (US 6,405,250) (hereinafter "Lin"). This rejection is traversed.

The claimed invention relates to a system and corresponding method for detecting the state of a computer network. As set forth in amended claim 2, the system includes:

> a plurality of distributed agents disposed in said computer network, each said agent comprising:
>
> data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;
>
> means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said computer network in a normal state and activities of said computer network in an abnormal state as a result of intrusions, infections, scams and/or other suspicious activities in said computer network; and
>
> means for comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models based on said collected data,
>
> wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

Claim 18 recites a corresponding method of detecting the state of a computer network. Such a system and method is not taught or suggested by Anderson and Lin taken separately or together.

In rejecting the claims over Anderson, the examiner now alleges that the directors 102 of Anderson correspond to the claimed "agents" and perform the functions of the "data collection means," "analyzing means," and "comparing means." In support of this position, the examiner cites to paragraph [0022] of Anderson, which notes that more than one director may be used that may relate to each other in a master/slave relationship, as peers, or in a hierarchy. Thus, unlike the previous official action where the claimed agents were identified as corresponding to sensors 104 (Figure 1), the examiner now alleges that the claimed agents correspond to directors 102. The examiner further alleges that Lin teaches developing activity models representative of the network in normal and abnormal states as claimed. Applicant disagrees and has amended the claims to clarify the distinctions over the prior art.

As previously noted, Anderson teaches the use of sensors 104 to collect network traffic data. Some or all of the sensors 104 may be integrally disposed with routing devices 106. One or more directors 102 (Figure 3) include an analyzer 304 and a regulator 306. As described in paragraph [0045] of Anderson, analyzer 304 analyzes the network traffic data from the sensors 104 and alerts regulator 306 which determines where and what actions to be taken. As noted in paragraph [0022] of Anderson, each director 102 is assigned responsibility for a subset of sensors 104 and selectively activates/deactivates the sensors 104 in addition to determining whether the network link of interest is suspicious of being abused or misused (for example, the source addresses of the network traffic routed over the network link of interest are even layered on top of the normal traffic pattern; see paragraph [0034]). As acknowledged by the examiner, the processing functions of Anderson are performed by the director 102.

In rejecting the claims over Anderson, the examiner alleges that Anderson develops activity models representative of activities of the network in a normal state and in an abnormal state. However, Anderson teaches receiving network traffic and determining whether the network link of interest is "at least suspicious of being abused or misused." Anderson says nothing of developing activity models. On the contrary, as disclosed in paragraph [0032] of Anderson, director 102 determines whether a network link is being misused by comparing the network traffic pattern depicted by the collected descriptive data against a set of "user-defined" thresholds for a "plurality of traffic pattern metrics." Anderson says nothing of comparing the collected data to "activity models representative of activities of said computer network in a normal state and activities of said computer network in an abnormal state as a result of intrusions, infections, scams and/or other suspicious activities in said computer network" as claimed. Anderson does not teach using such data collection and comparison techniques for identifying abnormal behavior as claimed.

As previously noted, Anderson does not teach comparing the results of the pattern analysis of data collected by one agent to the results of pattern analysis of data collected by analyzing means of other agents to "identify similar patterns of suspicious activity in different portions of the computer network" as claimed. Neither sensors 104 nor directors 102 are disclosed as performing any pattern analysis as claimed. In particular, Anderson does not teach that one director 102 compares the results of pattern analysis of data from a set of sensors 104 controlled by that director with the results of pattern analysis of data from another set of sensors controlled by another director to "identify similar patterns of suspicious activity in different portions of the computer network" as claimed. On the contrary, any "analysis" performed by the director 102 is for determining whether a network link of interest is "suspicious of being abused or misused." Anderson provides no way to extrapolate this finding to determine the status of the entire computer network as claimed.

Moreover, as acknowledged by the examiner at page 4 of the Official Action, Anderson "lacks or does not expressly disclose developing activity models representative of activities of said network" as claimed. For such teachings, the examiner refers to the general teachings of Lin of utilizing "behavior transition models" relating to network-wide behaviors leading to state transitions. Applicant submits that such models do not represent activities of the network in a "normal state" and activities of the network in an "abnormal state" for a determination by a comparing means as to whether the network is in a "normal state" or an "abnormal state" as claimed. Rather, Lin captures explanations of why the network moves from one state to another using a knowledge base based on the causal function h of all network elements (column 8, lines 1-13). There is no indication that such state transitions are based on detecting patterns of suspicious activity as claimed. Moreover, Lin specifically teaches away from the claimed methods by noting that there is "no way" for Lin's network management system to “passively observe” the behavior of a network element without the cooperation of the network element (column 6, lines 12-23).

Accordingly, neither Anderson nor Lin teaches a system that detects the state of a computer network, where the system comprises a “plurality of distributed agents” disposed in a computer network, where “each said agent” includes “comparing means” that “compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network” as claimed in independent claims 1 and 18. No such plural agents with such features are taught by Anderson and/or Lin. Directors 102 of Anderson are not disclosed as having such capabilities. The examiner’s conclusions to the contrary are not supported by the teachings of Anderson or Lin.

For at least these reasons, even if the teachings of Anderson and Lin could have been combined by one skilled in the art as the examiner alleged, the claimed system and method would not have resulted. The rejection of claims 2 and 18 as being unpatentable as obvious over Anderson in view of Lin is believed to be improper and withdrawal of this rejection is respectfully solicited. Claims 3-14, 16-17, and 19-21 are believed to be allowable as well at least by virtue of their dependencies upon claims 2 and 18, respectively.

Conclusion

For the reasons set forth herein, claims 2-14 and 16-21 are believed to be in condition for allowance. A Notice of Allowability is solicited.

Date: Monday, May 3, 2010

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439